

Dec. 2009



# Newsletter

**Utah Chapter**

*Our Mission: Provide our members opportunities for career development and networking with peers. Advance and promote the profession by creating awareness of the skills and abilities of IT audit and security Professionals.*

## President's Message

Greetings Utah Chapter members,

Hello Utah ISACA chapter members! We had a great November Fall Seminar; Cody Hatch presented on Securing the Borderless Network. It was a great seminar with great attendance. Thank you to Kyle Chugg and Brady Stevenson for putting together such a great seminar.

I am looking forward to seeing all of you at the December 17<sup>th</sup> meeting. We are lucky to have Michael Casey, Director of Information Security for Utah Department of Technology Services. He will be presenting on risk assessments / management.

We have our schedule booked up with great speakers and topics through May of 2010, so be sure to make room on your schedules to come to the events.

I hope all of your holiday preparations are going well, and I will see you at the Lion House on December 17th.

Thanks

Julie Park

### A Friendly Reminder:

It is that time of year to renew your ISACA annual membership! Please go to [ISACA.org](http://ISACA.org) to renew so you can enjoy the benefits of being an ISACA member all year long.

A BIG Thanks to Alan Sternecker for submitting articles for our monthly newsletter.

## Monthly Professional Training

Date: Thursday, Dec. 17th

Time: 11:30 – 1:15 pm.

Place: Lion House

Speaker: Michael Casey, Director of Information Security for Utah Department of Technology Services

Topic: Risk Assessments / Management

Cost: \$20 for members and \$15 for students, \$25 for non-members

CPE: 1 Credit

Email: [utah.isaca.chapter@gmail.com](mailto:utah.isaca.chapter@gmail.com)

Include the first and last name with e-mail address for each attendee you are registering.

Register at: <http://www.isaca-ut.org/utahevents.html>

### Menu

Sarah Salad

Chicken Swiss Bake

Chocolate Cream Cake

### Monthly Training Registration

The cutoff time period to sign up for the professional lunch meeting is the Tuesday before the monthly Thursday meeting. If you sign up after noon on Tuesday, you may or may not have a guaranteed seat. Since the rooms at the Lion House are small we have to give them a hard count by Tuesday at noon to reserve a room. Thanks

### Earning CPE

#### **ISACA e-Symposium**

\*\*\*\*\*

If you are in need of CPE credits, an easy way to earn them is by participating in an ISACA e-Symposium. These are free online web casts and you can earn 3 CPE credits. For further details, go to: [www.isaca.org/webcasts](http://www.isaca.org/webcasts)

I found out from ISACA that there is no limit to the number of e-Symposiums or on-line quizzes that you can take to help fulfill your CPE requirements. If you have any questions concerning CPE credits please email the following: [certification@isaca.org](mailto:certification@isaca.org) and they will answer your questions.

\*\*\*\*\*

## **Suggestions for Monthly Speakers**

If you have a topic you would like to hear in one of our monthly meetings or if you know of a good speaker please email Jackie Schwartz: [Jackie.Schwartz@usa.net](mailto:Jackie.Schwartz@usa.net)

## **Monthly Article**

### **Audit Checklists Their Use and Misuse**

A well managed IT audit program has robust plans, programs, procedures and most importantly committed staff members. Guiding these professionals are their work papers and integral to these documents are found their checklists. But how often have we received requests from fellow professionals seeking checklists for specialized audits for which they did not have relevant exemplars? These and similar events might introduce risks in audits that were unintended from the onset. Or in other cases, auditors examining audit activities used checklists applicable to outdated applications but continued to use them possibly overlooking vulnerabilities.

Audit checklists are not always required within management systems standards, however they constitute a valuable mechanism for auditors. Here are some areas (not intended to be all areas) where checklists might apply:

- Managers might like them as a tools anticipating audit costs.
- Organizations might like them as tools ensuring regulatory and legal compliance by auditors.
- Auditors might use them as a supports when dealing with security best practices.
- Auditors might use them to support their positions with regard to specialized procedural areas.
- Assure uniformity in the preparation of audit work papers by differing auditors.
- Assist auditors in meeting deadlines.

For example, auditing code checklists will not reveal all vulnerabilities especially as they might relate to the concepts of data classification and integrity. If the business requires data classification developers must understand how to ensure the availability, confidentiality and integrity of stored applications. During the development processes they must address the requirements of data storage, retrieval and secure transmission. As an observation, these same developers cannot merely "bolt on" encryption applications at the end of the development process and declare that it will work.

Needless to say developing most code is a complex process. And to add more complexity to the mixture, businesses have taken to outsourcing much of their application development to businesses outside their own country. So auditing code becomes even more important assuring that malicious code does not become part of the end-product.

Application specific checklists have been published on many Web sites by professionals making it simple for auditors to download them in a variety of platforms. But this is simply accepting the expertise of someone else hoping they have sufficiently covered the applicable scope of this particular audit. An audit manager or other relevant person may conclude that a checklist is sufficiently inclusive and that if followed all significant information security controls matters will be addressed. However, information security checklists placed in the hands of a well-trained security auditor will ensure more effective and efficient controls will be found or recommended. Consequently checklists are merely frameworks. Audit success depends on the auditor not the checklist.

In fact most organizations use checklists to ensure that audits are completed at a minimum level defined by the scope of the audit. Often serious misdeeds are found when auditors justify going off their checklists to find the heart of their work. One of the members of an audit team asked why one of the employees of an audit-target was driving a new luxury automobile when most of the other employees were not. This employee was a procurement clerk whose income did not support this vehicle. The audit manager assigned one of the most experienced auditors to review this employee's work and discovered a massive fraud conducted through the organization's computer system which would have gone undiscovered had it not been for the observation made by an auditor going off his checklist.

Checklists are used by pilots to ensure they have done everything at an acceptable level during flight preparation and landing. But if they see something wrong with the airplane's equipment that is not mentioned on the checklist the flight is aborted until corrective action is completed. Similarly auditors use checklists assuring that pertinent areas are reviewed. However if only the checklist is followed or if the auditor is unfamiliar with the areas addressed in the audit then there are risks introduced in the audit that are framed by the checklist alone. A reciprocal case is the auditor that strays off the checklist without sufficient justification and works aimlessly. This is another type of risk that enters audits wasting valuable resources and possibly creating needless managerial challenges.

A valuable managers' reference document for systems security auditing may be found at this link:  
<http://www.gao.gov/special.pubs/mgmtpln.pdf>. This document encompasses most of North America's relevant documentation having been produced as a joint state-federal effort.

Alan B. Sternecker, CISA, CISM, CFE, CISSP is a consultant and author of Critical Incident Management, ISBN: 084930010X, published by CRC Press, [www.crcpress.com](http://www.crcpress.com). He has written numerous articles and regularly lectures regarding fraud and computer systems security auditing. He can be reached at [absterneckert@yahoo.com](mailto:absterneckert@yahoo.com)

Happy Holidays!

## Board of Directors and Officers

**President**

Julie Park  
Weber State University  
[jpark@weber.edu](mailto:jpark@weber.edu)

**Vice President**

Jackie Schwartz  
Axiom Recovery  
[Jackie.Schwartz@usa.net](mailto:Jackie.Schwartz@usa.net)

**Treasurer**

Dan Walker  
Intermountain Health Care  
[Dan.Walker@imail.org](mailto:Dan.Walker@imail.org)

**Secretary**

Kyle Finlayson  
Intermountain Health Care  
[kyle.finlayson@intermountainmail.org](mailto:kyle.finlayson@intermountainmail.org)

**Newsletter/Publicity**

David Gibson  
Legislative Auditor General's Office  
[dgibson@utah.gov](mailto:dgibson@utah.gov)

**CISA Coordinator**

Jordan Fuller  
Amedica Corporation  
[jfuller@amedicacorp.com](mailto:jfuller@amedicacorp.com)

**Membership Director**

Michael Carter  
LDS Church  
[carterma@ldschurch.org](mailto:carterma@ldschurch.org)

**CISM Coordinator**

Brandon Greenwood  
XanGo  
[bgreenwood10@hotmail.com](mailto:bgreenwood10@hotmail.com)

**Seminar/Education Chair**

Kyle Chugg  
Questar  
[Kyle.Chugg@questar.com](mailto:Kyle.Chugg@questar.com)

**Academic Relations Chair**

Jeff Davis  
Weber State University  
[jtdavis@weber.edu](mailto:jtdavis@weber.edu)

**Research Chair**

Dan Anderson  
Intermountain Healthcare  
[Daniel.Anderson@imail.org](mailto:Daniel.Anderson@imail.org)

**Webmaster**

Ben West  
Protiviti  
[ben.west@protiviti.com](mailto:ben.west@protiviti.com)

The views and opinions contained in this publication are solely those of the authors, and do not necessarily represent or reflect the view or opinions of the Utah Chapter. In the event you have any questions concerning an article, you may wish to contact the author directly.

Happy